UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

DEIRDRE C. DONOVAN, BETH BYRD, KEVIN CURRAN, and ALLAN SPIELMAN, individually and on behalf of all others similarly situated, Plaintiffs, v. T-MOBILE USA, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Deirdre C. Donovan, Beth Byrd, Kevin Curran, and Allan Spielman ("Plaintiffs") bring this Class Action Complaint against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. T-Mobile is one of the three major cellular telephone carriers in the United States. As of the end of the second quarter of 2021, it had more than 104 million customers in the

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

United States.[1]

2. On or about August 15, 2021, Vice.com reported that hackers on the dark web were reporting that T-Mobile's entire (or nearly entire) customer dataset was for sale. Information that was being offered for sale included "social security numbers, phone numbers, names, physical addresses, unique IMEI numbers, and driver licenses information."[2] (This is personally identifiable information, or "PII.") Vice reported that it had seen samples of the data and that this information was, in fact, present and for sale.

3. Plaintiffs and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and IMEI numbers.

4. On August 18, 2021, T-Mobile confirmed the breach and unlawful access of its information (the "Data Breach"), but stated that only approximately 48 million records were stolen.[3] T-Mobile confirmed that names and Social Security numbers, dates of birth, and driver license numbers were stolen, but made no mention of IMEI numbers.

5. Not only did hackers steal the PII of Plaintiffs and Class members, but criminals have already sold or attempted to sell this information on the dark web. This stolen PII has great value to hackers. Because of Defendant's Data Breach, customers' PII is still available and may be for sale on the dark web for criminals to access and abuse. Defendant's customers face a current and ongoing lifetime risk of identity theft.

6. The information stolen in cyber-attacks allows the modern thief to assume your identity when carrying out criminal acts such as:

- Using your credit history.

---

[1] https://s24.q4cdn.com/400059132/files/doc_financials/2021/q2/NG_TMUS-06_30_2021-EX-99.1.pdf (last visited August 19, 2021).

[2] https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited August 19, 2021).

[3] https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2021/T-Mobile-Shares-Additional-Information-Regarding-Ongoing-Cyberattack-Investigation/default.aspx (last visited August 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

- Making financial transactions on your behalf, including opening credit accounts in your name.
- Impersonating you via mail and/or email.
- Impersonating you in cyber forums and social networks.
- Stealing benefits that belong to you.
- Stealing your smartphone's data, through a SIM-swap attack.
- Committing illegal acts which, in turn, incriminate you.

7. Plaintiffs' and Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class members.

8. As of this writing, there exist many class members who have no idea their PII has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect consumers' PII, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL"); the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. (the "CCPA"); California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA"); Illinois' Consumer Fraud and Deceptive Business Practices

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Act, 815 ILCS 505/1, *et seq.* (the "ICFA"); and New York's General Business Law §§ 349, 350, *et seq*. (the "NYGBL"); and (v) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

PARTIES

11. Plaintiff Deirdre C. Donovan is a citizen of California, residing in San Francisco County, California. As a current T-Mobile customer for three years, Ms. Donovan believes her PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach. T-Mobile confirmed in a text message to Ms. Donovan that her PII was stolen in the Data Breach.

12. Plaintiff Beth Byrd is a citizen of California, residing in San Diego County, California. As a current T-Mobile customer for at least three years, Ms. Byrd believes her PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach. T-Mobile confirmed in a text message to Ms. Byrd that her PII was stolen in the Data Breach.

13. Plaintiff Kevin Curran is a citizen of Illinois, residing in Cook County. As a current T-Mobile customer and for the past approximately 18 years, Mr. Curran believes his PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach. T-Mobile confirmed in a text message to Mr. Curran that his PII was stolen in the Data Breach.

14. Plaintiff Allan Spielman is a citizen of New York, residing in Nassau County. As a current T-Mobile customer and for the at least the past 5 years, Mr. Spielman believes his PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach.

15. Defendant T-Mobile USA, Inc. is a Delaware corporation with its principal place of business at 12920 SE 38th St., Bellevue, Washington. It is a publicly-traded company, though a majority of its stock is held by Deutsche Telekom and the Softbank Group. As of January 1, 2021, Defendant had annual gross revenues of well over $60 billion. Defendant collects and maintains the personal information of millions of U.S. and California consumers.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

17. This Court has personal jurisdiction over Defendant because Defendant's principal places of business are located within this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

19. T-Mobile (as a result of the 2020 merger with Sprint Communications) is the second-largest cellular service provider in the United States. It recently reported having 104.8 million subscribers.

20. In the ordinary course of doing business with Defendant, customers and prospective customers are required to provide Defendant with sensitive PII such as:

a. Contact and account information, such as name, usernames, passwords, address, telephone number, email address, and household members;

b. Authentication and security information such as government identification, Social Security number, security codes, and signature;

c. Demographic information, such as age, gender, veteran status, and date of birth;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

d. Payment information, such as credit card, debit card, and bank account number; and

e. Preference information, including preferences related to marketing, advertising and communications and participation in T-Mobile programs.[4]

21. Defendant also automatically collects the following information from its customers:

a. Customer Proprietary Network Information ("CPNI") generated by use of T-Mobile's wireless voice communications services;

b. Unique identifiers like cookie IDs, device IDs including mobile advertising IDs, IP address, and media access control ("MAC") address collected though tracking technologies like web beacons, pixels, and other tracking technologies;

c. Information from use of T-Mobile's products, services, and network (and other carriers' networks when roaming domestically or internationally) like a customer's usage of connecting carriers and Internet service providers, the Internet Protocol ("IP") address, text messages, and data use history, websites and URLs visited, content interactions (e.g., how long customers use an app), viewing info from our streaming services (e.g., videos customers watch on TVision), mobile apps installed or used or that interact with customers' devices, language settings, and other network and device analytics and Wi-Fi connection and usage data;

d. Device and service performance and diagnostic information, including reports from customer devices about signal strength, speeds, app and service performance, dropped calls, call and data failures, geolocation information, and device data like battery strength and serial number and

[4] https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited August 20, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

similar device identifiers, settings, language preferences, and software versions, including customer browser type and operating system version, the website that referred the customer to one of T-Mobile's websites, or that a customer visits upon leaving its websites.

e. Back-up information, including data stored in back-ups and cloud services if the customer device uploads information to T-Mobile network servers (e.g., some devices may back-up a customer's address book, photo album, or diagnostic data);

f. Commercial information, including records of customer purchases from T-Mobile and purchase tendencies;

g. Geolocation data, specifically data that identifies the approximate or precise location of a customer's mobile device. T-Mobile may also use location technologies to collect data about the presence of a customer's device;

h. Biometric data, including biometric signatures for authentication and fraud prevention.

i. Video data, including images from video monitoring and recordings of people in T-Mobile's retail stores;

j. Audio information, including voice commands customers provide to T-Mobile's apps (for example, for accessibility or hands-free use), and audio recordings of calls between customers and T-Mobile's customer service representatives.[5]

22. In addition to the types of information Defendant collects from consumers listed above, Defendant collects personal information through consumer reporting agencies, financial institutions, social media platforms, analytics providers, and consumer data resellers. This

[5] *Id.*

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

personal information includes contact information, demographic information, geolocation information, and information about consumers' interests, preferences, or behaviors.[6]

23. Defendant represents on its website:

> The collection and use of your personal data is critical to the operations of most modern organizations—including T-Mobile. We collect information required to open and service your account. We also collect and use personal data about you for a variety of business and commercial purposes such as, but not limited to: providing you customer service and technical assistance on our Products or Services (as those terms are defined in our Privacy Notice), processing orders and payments, ***detecting and protecting you against security incidents and illegal or unauthorized activities***, and understanding your interests and behaviors to customize your experiences through personalized content and advertisements for specific products and offers."[7]

24. Additionally, when opening an account with T-Mobile, every customer is issued an IMEI number, which is "a unique number for identifying a device on a mobile network. You can think of it as your phone's social security number. It has 15 digits and is assigned to every GSM phone."[8] T-Mobile, like most carriers, uses GSM network standards.

25. IMEI numbers "could potentially be used to track the location of mobile devices or be used in SIM swapping attacks that could aid bad actors in bypassing multi-factor authentication for accounts."[9]

The Data Breach

26. On or about August 15, 2020, Vice.com first reported that T-Mobile was investigating a "forum post claiming to be selling a mountain of personal data."[10]

27. This reported further noted:

---

[6] *Id.*

[7] https://www.t-mobile.com/privacy-center/support#faq (last visited August 20, 2021) (emphasis added).

[8] https://www.androidauthority.com/what-is-imei-923061/ (last visited August 20, 2021).

[9] https://appleinsider.com/articles/21/08/20/t-mobile-says-53m-more-customers-affected-by-breach-imei-data-stolen (last visited August 20, 2021).

[10] https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited August 20, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

> . . . the seller told Motherboard they have obtained data related to over 100 million people, and that the data came from T-Mobile servers.
>
> The data includes social security numbers, phone numbers, names, physical addresses, unique IMEI numbers, and driver licenses information, the seller said. Motherboard has seen samples of the data, and confirmed they contained accurate information on T-Mobile customers.[11]

28. Security blogger Alon Gal ("Under the Breach") states that he spoke to the hackers responsible, who stated that the Data Breach was "done to retaliate against the US for the kidnapping and torture of John Erin Binns . . . by CIA and Turkish agents in 2019" and that it was done "to hard US infrastructure."[12]

29. Notwithstanding the hackers' motivations, "[o]n the underground forum the seller is asking for 6 bitcoin, around $270,000, for a subset of the data containing 30 million social security numbers and driver licenses. The seller said they are privately selling the rest of the data [of 70+ million customers] at the moment."[13]

30. T-Mobile initially represented on August 17th that approximately 47.8 million people were affected, but by August 20th, that number had increased to 53.8 million.[14] T-Mobile as yet has not refuted the hacker's claims that virtually the entire customership of T-Mobile was exfiltrated, nor has it given any assurances that it has identified the entire scope of the exfiltration.

31. Any Class member who saw the August 2021 media reports on the subject but who did not receive any Notice of Data Breach likely concluded that their data was not impacted in the Data Breach and therefore would not have known of the need to take action to protect themselves.

---

[11] *Id.*

[12] https://twitter.com/UnderTheBreach/status/1426923538099970050 (last visited August 20, 2021).

[13] https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited August 20, 2021).

[14] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last visited August 20, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

32. Additionally, Consumer Reports noted that "T-Mobile has created a web page with up-to-date information and remedies for consumers. The page does not offer a way to determine whether your account is one of those affected by the breach."[15] As of this writing, this continues to be true.

33. Notably, T-Mobile has, in just the past three years, been the target of ***five*** additional data breaches.[16] In 2015, T-Mobile was also the subject of the Experian Data Breach, which led to the exfiltration of the financial information of 15 million people who had applied for phones through T-Mobile and who required a credit check as part of the process.[17] The Experian Data Breach led to a more than $40 million class action settlement[18], and put T-Mobile on more than adequate notice of the value of its customers' data.

34. T-Mobile has offered two years of McAfee ID Theft Protection Service, but it is unclear who is eligible to sign up for it.[19]

Defendant Was Aware of the Risks of a Data Breach

35. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

36. Plaintiffs and Class members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the cellular communications services

---

15 https://www.consumerreports.org/data-theft/t-mobile-data-breach-what-to-do-a7157173229/ (last visited August 20, 2021).

16 *Id.*

17 https://www.t-mobile.com/news/blog/experian-data-breach (last visited August 20, 2021).

18 https://www.expdatabreachsettlement.com/ (last visited August 20, 2021).

19 https://www.t-mobile.com/brand/data-breach-2021/next-steps?icid=MGPO_TMO_U_21DTASECRT_AH73WUMF4XHQD39VY26095 (last visited August 20, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

industry preceding the date of the breach.

38. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

39. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[20] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[21]

40. The PII of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and members of the Class, including Social Security numbers, driver license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and members of the Class a result of a breach.

42. Plaintiffs and members of the Class now face years of constant surveillance of

---

[20] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited August 22, 2021).

[21] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

43. The injuries to Plaintiffs and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and members of the Class.

Defendant Failed to Comply with FTC Guidelines

44. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

45. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

47. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"),

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Comply with Industry Standards

49. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

50. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

51. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

52. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

The Value of PII to Cyber Criminals

53. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

54. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[22]

55. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

56. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective. According to Julie

---

[22] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited August 22, 2021).

[23] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited August 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

58. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[25]

59. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiffs and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the Class. Stolen personal data of Plaintiffs and members of the Classes represents essentially one-stop shopping for identity thieves.

60. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection

[24] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited August 22, 2021).

[25] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited August 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

programs, monitoring data traffic, and having in place a response plan.

61. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

62. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiffs and members of the Class has a high value on both legitimate and black markets.

63. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

64. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

65. Based on the foregoing, the information compromised in the Data Breach is

[26] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited August 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[27]

67. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiffs' and Class Members' Damages

68. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered twenty-four months of identity monitoring services, which is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

69. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class members' PII.

---

[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited August 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

70. Plaintiffs and Class members have been damaged by the compromise of their PII in the Data Breach.

71. Plaintiffs and Class members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

72. Plaintiffs and Class members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegal based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class members.

73. Plaintiffs and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

74. Plaintiffs and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

75. Plaintiffs and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

76. Plaintiffs and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

77. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

78. Further, as a result of Defendant's conduct, Plaintiffs and Class members are

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

79. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

80. Plaintiffs bring this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose PII was compromised in the Data Breach announced on or about August 15, 2021 (the "Nationwide Class").

81. The California Subclass is defined as follows:

> All natural persons residing in California whose PII was compromised in the Data Breach announced on or about August 15, 2021 (the "California Subclass").

82. The Illinois Subclass is defined as follows:

> All natural persons residing in Illinois whose PII was compromised in the Data Breach announced on or about August 15, 2021 (the "Illinois Subclass").

83. The New York Subclass is defined as follows:

> All natural persons residing in New York whose PII was compromised in the Data Breach announced on or about August 15, 2021 (the "New York Subclass").

84. The California, Illinois, and New York Subclasses are collectively referred to herein as the "Statewide Subclasses," and, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

85. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

86. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

87. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has indicated that the PII of hundreds of thousands of individuals has been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

88. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiffs and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiffs and members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the PII of Plaintiffs and members of the Classes secure and to prevent loss or misuse of that PII;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiffs and the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and members of the Classes that their PII had been

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

compromised;

j. Whether Plaintiffs and the other members of the Classes are entitled to credit monitoring and other monetary relief;

k. Whether Defendant violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL");

l. Whether Defendant violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. (the "CCPA");

m. Whether Defendant violated California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA"); and

n. Whether Defendant violated Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* (the "ICFA"); and

o. Whether Defendant violated New York's General Business Law §§ 349, 350, *et seq.* (the "NYGBL").

89. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Classes because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

90. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs' counsel are competent and experienced in litigating privacy-related class actions.

91. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

92. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to each of the Statewide Subclasses as a whole.

93. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF

Negligence

(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses)

94. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

95. Defendant owed a duty to Plaintiffs and the members of the Classes to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

96. The legal duties owed by Defendant to Plaintiffs and the members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and members of the Classes in their possession;

b. To protect PII of Plaintiffs and members of the Classes in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and members of the Classes of the Data Breach.

97. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

98. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

99. Defendant breached its duties to Plaintiffs and members of the Classes. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

100. Defendant knew or should have known that their security practices did not adequately safeguard the PII of Plaintiffs and the other members of the Classes.

101. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiffs and the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant's unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and other members of the Classes during the period it was within Defendant's possession and control.

102. Defendant breached the duties they owe to Plaintiffs and members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

103. Due to Defendant's conduct, Plaintiffs and members of the Classes are entitled to identity theft protection. The PII taken can be used for identity theft and other types of financial fraud against the members of the Classes.

104. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

105. As a result of Defendant's negligence, Plaintiffs and members of the Classes suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and members of the Classes, including ongoing credit monitoring.

106. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiffs and the other members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

SECOND CLAIM FOR RELIEF

Negligence *Per Se*

(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses)

107. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

108. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

109. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and members of the Classes due to the valuable nature of the PII at issue in this case—including Social Security numbers.

110. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

111. Plaintiffs and members of the Classes are within the class of persons that the FTC Act was intended to protect.

112. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Classes.

113. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and members of the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current and former customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and members of the Classes.

114. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unlawful Business Practices
(On Behalf of Plaintiffs Deirdre C. Donovan and Beth Byrd and the Nationwide Class or, in the Alternative, the California Subclass)

115. Plaintiffs Donovan and Byrd re-allege and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

116. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class or, in the alternative, the California Subclass.

117. Defendant engaged in unlawful acts and practices with respect to its services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff Donovan's, Plaintiff Byrd's and the Nationwide Class' and California Subclass' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff Donovan's, Plaintiff Byrd's, the Nationwide Class' and California Subclass' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class and California Subclass members. Defendant also violated: the California Consumer

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. and the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., as alleged below; and also the California Financial Information Privacy Act, California Financial Code § 4052.5; the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; and Article 1, § 1 of the California Constitution.

118. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the data breach to Nationwide and California Subclass members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendant still has not provided such information to Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class and California Subclass.

119. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class and California Subclass were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Nationwide Class' and California Subclass' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

120. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Nationwide Class' and California Subclass' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide Class and California Subclass.

121. Nationwide Class and California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class and the California Subclass of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

FOURTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unfair Business Practices
(On Behalf of Deirdre C. Donovan, Plaintiff Byrd and the Nationwide Class or, in the Alternative, the California Subclass)

122. Plaintiff Donovan and Plaintiff Byrd re-allege and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

123. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the Nationwide Class' and California Subclass' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff Donovan's, Plaintiff Byrd's, the Nationwide Class' and the California Subclass' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and the California Subclass. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiff Donovan, Plaintiff Byrd's, Plaintiff Byrd, Plaintiff Byrd, the Nationwide Class, and the California Subclass outweighed their utility, if any.

124. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff Donovan's, Plaintiff Byrd's, the Nationwide Class', and California Subclass' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and the California Subclass. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and the California Subclass outweighed their utility, if any.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

125. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and the California Subclass were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Nationwide Class', and California Subclass' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

126. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Donovan's, Plaintiff Byrd's, the Nationwide Class', and the California Subclass' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and California Subclass.

127. Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and the California Subclass seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff Donovan, Plaintiff Byrd, the Nationwide Class, and the California Subclass of money or property that the Defendant may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

FIFTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*.
(On Behalf of Plaintiff Deirdre C. Donovan and Beth Byrd and the California Subclass)

128. Plaintiffs Donovan and Byrd re-allege and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

129. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Donovan's, Plaintiff Byrd's and the California Subclass' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Donovan, Plaintiff Byrd and the California Subclass.

130. As a direct and proximate result of Defendant's acts, Plaintiff Donovan's, Plaintiff Byrd's, and the California Subclass' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through T-Mobile's computer systems and/or from the dark web, where hackers further disclosed T-Mobile's customers' PII.

131. As a direct and proximate result of Defendant's acts, Plaintiff Donovan, Plaintiff Byrd and the California Subclass were injured and lost money or property, including but not limited to the price received by Defendant for its services, the loss of Plaintiff Donovan's, Plaintiff Byrd's and the California Subclass' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

132. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Donovan's, Plaintiff Byrd's and the California Subclass' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff Donovan, Plaintiff Byrd and the California Subclass.

133. Defendant T-Mobile is a public company that is organized or operated for the profit or financial benefit of its shareholders, with revenues of well over 60 billion. T-Mobile collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

134. At this time, Plaintiff Donovan, Plaintiff Byrd and the California Subclass seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs, and any other relief the court deems proper.

135. Concurrently with the filing of this complaint, Plaintiffs Donovan and Byrd provided written notice to Defendant identifying the specific provisions of this title she alleges it

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

has violated. Assuming Defendant does not cure the Data Breach within 30 days, and Plaintiffs Donovan and Byrd believe any such cure is not possible under these facts and circumstances, Plaintiff Donovan and Byrd intend to amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

SIXTH CLAIM FOR RELIEF

Violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*.
(On Behalf of Plaintiffs Deirdre C. Donovan and Beth Byrd and the California Subclass)

136. Plaintiffs Donovan and Byrd re-allege and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

137. The California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. ("CLRA"), was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendant's acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Defendant's communications services are intended to and did result in sales of those communications services.

138. Plaintiffs Donovan and Byrd and the other California Subclass members are consumers within the meaning of Cal. Civ. Code §1761(d).

139. Defendant's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of the Network and deceptively representing that it adequately maintained such information, Defendant violated the CLRA. Defendant had exclusive knowledge of undisclosed material facts, namely, that its network was defective and/or unsecure, and withheld that knowledge from Plaintiffs Donovan and Byrd and the California Subclass.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

140. Defendant's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of section 1770 the CLRA, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

For purposes of the CLRA, omissions are actionable along with representations.

141. Defendant stored Plaintiff Donovan's, Plaintiff Byrd's, the California Subclass' PII on its network. Defendant represented to Plaintiffs Donovan and Byrd and the California Subclass that its network was secure and that their PII would remain private. Defendant engaged in deceptive acts and business practices by providing in its Privacy Policy: "We use administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control."[28]

142. Defendant knew or should have known that it did not employ reasonable measures that would have kept Plaintiff Donovan's, Plaintiff Byrd's and the California Subclass' PII secure and prevented the loss or misuse of their PII. For example, Defendant failed to take

[28] https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited Aug. 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

reasonable steps to prevent the loss of PII through its servers through appropriate encryption and industry best practices.

143. Defendant's deceptive acts and business practices induced California Subclass members to provide PII, including Social Security numbers and driver license numbers, for the purchase of communications services. But for these deceptive acts and business practices, California Subclass members would not have purchased communication services, or would not have paid the prices they paid for the communication services.

144. Defendant's representations that it would secure and protect California Subclass members' PII in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase communication services.

145. California Subclass members were harmed as the result of Defendant's violations of the CLRA, because their PII was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their PII; and their PII was disclosed to third parties without their consent.

146. California Subclass members suffered injury in fact and lost money or property as the result of Defendant's failure to secure their PII; the value of their PII was diminished as the result of Defendant's failure to secure their PII; and they have expended time and money to rectify or guard against further misuse of their PII.

147. Defendant's conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

148. As the result of Defendant's violations of the CLRA, Plaintiffs Donovan and Byrd, on behalf of themselves, California Subclass members, and the general public of the State of California, seeks injunctive relief prohibiting Defendant from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendant's conduct violated the CLRA.

149. Pursuant to Cal. Civ. Code § 1782, concurrently with the filing of this complaint, Plaintiffs Donovan and Byrd mailed Defendant notice in writing, via U.S. certified mail, of its

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

particular violations of Cal. Civ. Code § 1770 of the CLRA and demanded that it rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendant's legal obligations, and to give notice to all affected customers of its intent to do so. If Defendant fails to respond to the letter within 30 days and to take the actions demanded to rectify its violations of the CLRA, Plaintiffs Donovan and Byrd will amend this complaint to seek damages and attorneys' fees as allowed by the CLRA.

SEVENTH CLAIM FOR RELIEF
Violation of the Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*. (the "ICFA")
(On Behalf of Plaintiff Kevin Curran and the Illinois Subclass)

150. Plaintiff Curran re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

151. Plaintiff Curran and the Illinois Subclass are "consumers" as that term is defined in 815 Ill. Comp. Stat. § 505/1(e).

152. Plaintiff Curran, the Illinois Subclass, and T-Mobile are "persons" as that term is defined in 815 Ill. Comp. Stat. § 505/1(c).

153. T-Mobile is engaged in "trade" or "commerce," including provision of services, as those terms are defined under 815 Ill. Comp. Stat. § 505/1(f).

154. T-Mobile engages in the "sale" of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

155. T-Mobile engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ICFA) in violation of the ICFA, including but not limited to the following:

a. failing to maintain sufficient security to keep Plaintiff Curran's and the Illinoi Subclass' sensitive PII from being hacked and stolen; and

b. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Curran and the

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Illinois Subclass Members' PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

156. In addition, T-Mobile's failure to disclose that its computer systems were not well-protected and that Plaintiff Curran's and the Illinois Subclass' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because T-Mobile knew such facts would (a) be unknown to and not easily discoverable by Plaintiff Curran and the Illinois Subclass; and (b) defeat Plaintiff Curran and the Illinois Subclass' ordinary, foreseeable and reasonable expectations concerning the security of their PII on T-Mobile servers.

157. T-Mobile intended that Plaintiff Curran and the Illinois Subclass rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with T-Mobile's offering of goods and services and incorporating Plaintiff Curran's and the Illinois Subclass' PII on its servers, in violation of the ICFA.

158. T-Mobile also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiff Curran's and the Illinois Subclass' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

159. T-Mobile's wrongful practices occurred in the course of trade or commerce.

160. T-Mobile's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of T-Mobile that applied to Plaintiff Curran and all Illinois Subclass members and were repeated continuously before and after T-Mobile obtained sensitive PII and other information from Plaintiff Curran and the Illinois Subclass. Plaintiff Curran and the Illinois Subclass were adversely affected by T-Mobile's conduct and the public was and is at risk as a result thereof.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

161. T-Mobile also violated 815 Ill. Comp. Stat. § 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. § 530/45, *et. seq*., which provides:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

162. 815 Ill. Comp. Stat. § 530/20 provides that a violation of 815 Ill. Comp. Stat. § 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

163. As a result of T-Mobile's wrongful conduct, Plaintiff Curran and the Illinois Subclass were injured in that they never would have allowed their sensitive PII – the value over which Plaintiff Curran and the Illinois Subclass no longer have control – to be provided to T-Mobile if they had been told or knew that T-Mobile failed to maintain sufficient security to keep such data from being hacked and taken by others.

164. T-Mobile's unfair and/or deceptive conduct proximately caused Plaintiff Curran and the Illinois Subclass' injuries because, had T-Mobile maintained customer PII with adequate security, Plaintiff Curran and the Illinois Subclass would not have lost it.

165. As a direct and proximate result of T-Mobile's conduct, Plaintiff Curran and the Illinois Subclass have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made from T-Mobile that Plaintiff Curran and the Illinois Subclass would have never made had they known of T-Mobile's careless approach to cybersecurity; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

in an amount to be proven at trial.

166. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Curran and the Illinois Subclass seek actual, compensatory, and punitive damages (pursuant to 815 Ill. Comp. Stat. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of T-Mobile's violations of the ICFA.

EIGHTH CLAIM FOR RELIEF
Violation of New York's General Business Law § 349, *et seq*.
(On Behalf of Plaintiff Allan Spielman and the New York Subclass)

167. Plaintiff Spielman re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

168. New York's General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.

169. In its provision of services throughout the State of New York, Defendant conducts business and trade within the meaning and intendment of New York's General Business Law § 349.

170. Plaintiff Spielman and members of the New York Subclass are consumers who conducted transactions with Defendant for their personal use.

171. As outlined above, Defendant engaged in deceptive acts and practices in the conduct of its business and in the furnishing of its services, including failing to implement adequate data security measures, failing to protect Plaintiff Spielman's and the New York Subclass' PII from theft, failing to advise Plaintiff Spielman and the New York Subclass of its inadequate data security, and failing to timely notify Plaintiff Spielman and the New York Subclass of the breach.

172. By the acts and conduct alleged herein, Defendant has engaged in deceptive, unfair, and misleading acts and practices, which include, without limitation, misrepresenting that Defendant used "administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control."

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

173. The foregoing deceptive acts and practices were directed at consumers and, thus, constituted "consumer-oriented conduct" under § 349.

174. The foregoing deceptive acts and practices are misleading in a material way b because they fundamentally misrepresent the ability and measures taken by Defendant to safeguard consumer PII, and to induce consumers to enter transactions with Defendant.

175. Plaintiff Spielman and the New York Subclass relied on Defendant to safeguard their PII when they provided it to WMG and relied on WMG's deceptive acts and practices when they provided that PII in exchange for Defendant's goods and services.

176. By reason of this conduct, Defendant engaged in deceptive conduct in violation of GBL § 349.

177. Defendant's actions are the direct, foreseeable, and proximate cause of the damages that Plaintiff Spielman and members of the New York Subclass have sustained from having provided their PII to Defendant, which was exposed in the Data Breach. As a result of Defendant's violations, Plaintiff Spielman and the New York Subclass have suffered damages because: (a) they would not have provided their PII to Defendant had they known Defendant did not use "administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control"; (b) they have suffered identity theft and/or fraudulent charges and their PII has been devalued as a result of being exposed in the Data Breach; and (c) Plaintiff Spielman and members of the New York Subclass must spend considerable time and expenses dealing with the effects of the Data Breach, and they now face a present and imminent lifetime risk of identity theft stemming from the Data Breach.

178. On behalf of himself and other members of the New York Subclass, Plaintiff Spielman seeks to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

NINTH CLAIM FOR RELIEF
Violation of Violation of New York General Business Law, § 350, *et seq*.
(On Behalf of Plaintiff Allan Spielman and the New York Subclass)

179. Plaintiff Spielman re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

180. New York's General Business Law § 350 prohibits false advertising in the conduct of any business, trade, or commerce.

181. Pursuant to said statute, false advertising is defined as "advertising, including labeling, of a commodity ... if such advertising is misleading in a material respect."

182. Based on the foregoing, Defendant has engaged in consumer-oriented conduct that is deceptive or misleading in a material way which constitutes false advertising in violation of GBL § 350.

183. Defendant's false, misleading, and deceptive statements and representations of fact were and are directed to consumers.

184. Defendant's false, misleading, and deceptive statements and representations of fact were and are likely to mislead a reasonable consumer acting reasonably under the circumstances.

185. Defendant's false, misleading, and deceptive statements and representations of fact have resulted in consumer injury or harm to the public interest.

186. As a result of Defendant's false, misleading, and deceptive statements and representations of fact, Plaintiff Spielman and the New York Subclass have suffered and continue to suffer economic injury.

187. As a result of Defendant's violations, Plaintiff Spielman and members of the New York Subclass have suffered damages due to said violation because: (a) they would not have provided their PII to Defendant had they known Defendant did not use "administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control;" (b) they have suffered identity theft and/or fraudulent charges and their PII has been devalued as a result of being exposed in the Data Breach; and (c) Plaintiff Spielman and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

members of the New York Subclass must spend considerable time and expenses dealing with the effects of the Data Breach and they now face a present and imminent lifetime risk of identity theft stemming from the Data Breach.

188. On behalf of himself and other members of the New York Subclass, Plaintiff Spielman seeks to recover their actual damages or five hundred dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

TENTH CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses)

189. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

190. When Plaintiffs and Nationwide Class members provided their PII to Defendant in exchange for Defendant's products and services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their PII.

191. Defendant solicited and invited Plaintiffs and the Nationwide Class to provide their PII as part of Defendant's regular business practices and as essential to the sales transactions entered into between Defendant on the one hand and Plaintiffs and Nationwide Class members on the other. This conduct thus created implied contracts between Plaintiffs and Nationwide Class members on the one hand, and Defendant on the other hand. Plaintiffs and Nationwide Class members accepted Defendant's offers by providing their PII to Defendant in connection with their purchases from Defendant.

192. When entering into these implied contracts, Plaintiffs and Nationwide Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

193. Defendant's implied promise to safeguard Plaintiffs' and Nationwide Class members' PII is evidenced by a duty to protect and safeguard PII that Defendant required

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Plaintiffs and Nationwide Class members to provide as a condition of entering into consumer transactions with Defendant.

194. Plaintiffs and Nationwide Class members paid money to Defendant to purchase products or services from Defendant. Plaintiffs and Nationwide Class Members reasonably believed and expected that Defendant would use part of funds received as a result of the purchases to obtain adequate data security. Defendant failed to do so.

195. Plaintiffs and Nationwide Class members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from customers' continued use of Defendant's communications services—that Defendant would adequately safeguard PII. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and Nationwide Class members.

196. Plaintiffs and Nationwide Class members value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

197. Plaintiffs and Nationwide Class members fully performed their obligations under their implied contracts with Defendant.

198. Defendant breached its implied contracts with Plaintiffs and Nationwide Class members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

199. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Nationwide Class members sustained damages as alleged herein.

200. Plaintiffs and Nationwide Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

201. Plaintiffs and Nationwide Class members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiffs and Nationwide Class members.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

ELEVENTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses)

202. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

203. Defendant owes duties of care to Plaintiffs and Nationwide Class members which require it to adequately secure their PII.

204. Defendant still possess Plaintiffs' and Nationwide Class members' PII.

205. Defendant has not specified what steps it has taken to prevent a data breach from occurring again.

206. Plaintiffs and Nationwide Class members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

207. Plaintiffs, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Nationwide Class members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

TWELFTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses)

208. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

209. Defendant benefited from receiving Plaintiffs' and Nationwide Class members' PII by their ability to retain and use that information for its own benefit. Defendant understood this benefit.

210. Defendant also understood and appreciated that Plaintiffs' and Nationwide Class members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

211. Plaintiffs and Nationwide Class members who were customers of Defendant conferred a monetary benefit upon Defendant in the form of monies paid for services from Defendant.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

212. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Nationwide Class members. Defendant also benefited from the receipt of Plaintiffs' and Nationwide Class members' PII, as Defendant used it to facilitate the transfer of information and payments between the parties.

213. The monies that Plaintiffs and Nationwide Class members paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

214. Defendant also understood and appreciated that Plaintiffs' and Nationwide Class members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

215. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted with Defendant. Indeed, if Defendant had informed Plaintiffs and Nationwide Class members that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

216. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Nationwide Class members. Defendant continues to benefit and profit from its retention and use of the PII while its value to Plaintiffs and Nationwide Class Members has been diminished.

217. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiffs' and Nationwide Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

218. As a result of Defendant's conduct, Plaintiffs and Nationwide Class members suffered actual damages in an amount equal to the difference in value between the amount Plaintiffs and Nationwide Class members paid for their purchases with reasonable data privacy

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

219. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Nationwide Class members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Nationwide Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

220. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Nationwide Class members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Nationwide Class members and Statewide Subclass members, request judgment against Defendant and that the Court grant the following:

A. An order certifying the Classes as defined herein, and appointing Plaintiffs and their counsel to represent the Classes;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiffs and the members of the Classes;

C. An order requiring Defendant to:

a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engage third-party security auditors and internal personnel to run automated security monitoring;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

c. Audit, test, and train their security personnel regarding any new or modified procedures;

d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiffs and Nationwide Class members for a period of ten years; and

h. Meaningfully educate Plaintiffs and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

D. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all members of the Classes;

E. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

F. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

G. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

RESPECTFULLY SUBMITTED AND DATED this 23rd day of August, 2021.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 N. 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 206-816-6603
Facsimile: (206) 319-5450

Betsy C. Manifold*
Rachele R. Byrd*
Email: byrd@whafh.com
Marisa C. Livesay*
Brittany N. Dejong*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, California 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599

Carl V. Malmstrom*
Email: malmstrom@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Telephone: (312) 984-0000
Facsimile: (212) 545-4653

Attorneys for Plaintiffs and the Class

* *Pro Hac Vice Application Forthcoming*